<EXAM NAME> Penetration Testing Report

<CLIENT NAME HERE>

By

<NAME HERE>

Version 1.0

Copyright © <YOUR NAME>

Table of Contents

Confidentiality Statement....3
Disclaimer....3
Contact Information....3
Assessment Overview....4
Assessment Components....4
External Penetration Test....4
Internal Penetration Test....4
Web Application Penetration Test....4
Risk Factors....7
Likelihood....7
Impact....7
Scope....7
Scope Exclusions....7
Client Allowances....7
Executive Summary....8
Testing Summary....8
Security Strengths....8
Strength....8
Strength....8
Security Weaknesses....8
Weakness....9
Weakness....9
Weakness....9
Penetration Test Findings....10
IPT:001 – Finding Name....10
WPT:002 – Finding Name....11
EPT:003 – Finding Name....12

Copyright © <YOUR NAME>

Confidentiality Statement

This document is the exclusive property of <CLIENT NAME> and <YOUR NAME>. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both <CLIENT> and <YOUR NAME>.

<YOUR NAME> may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. <YOUR NAME> prioritized the assessment to identify the weakest security controls an attacker would exploit. <YOUR NAME> recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
<CLIENT BUSINESS NAME>		
John Smith	CISO – <CLIENT>	Office: (555) 555-5555 Email: john.smith@demo.com
<YOUR NAME>		
<YOUR NAME>	Lead Penetration Tester	Email : YOUR EMAIL

Copyright © <YOUR NAME>

Assessment Overview

From <START DATE> to <END DATE>, <CLIENT> engaged <YOUR NAME> to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. An engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Web Application Penetration Test

A web application penetration test is an in-depth penetration test on both the unauthenticated and authenticated portions of your website. The engineer will test for all the OWASP Top-10 critical security flaws, as well as a variety of other potential vulnerabilities based on security best practice. Activities include website mapping, directory enumeration, automated and manual injection testing, directory traversal testing, malicious file uploads and remote code execution, password attacks and

Copyright © <YOUR NAME>

authentication bypasses, session attacks, and other testing depending on specific site content and languages.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9-10	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7-8	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4-6	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	1-3	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Copyright © <YOUR NAME>

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
<ASSESSMENT TYPE HERE>	<IP ADDRESSES, HOSTNAMES, ETC>

Scope Exclusions

Per client request, <CLIENT NAME> did not perform any of the following attacks during testing:

- **Scope exclusion here**

All other attacks not specified above were permitted by <CLIENT>.

Client Allowances

<CLIENT> provided <YOUR NAME> the following allowances:

Copyright © <YOUR NAME>

- **Scope allowance here**

Copyright © <YOUR NAME>

Executive Summary

<YOUR NAME> evaluated <CLIENT>'s exam security posture through a <EXAM TYPE> penetration test from <START DATE> through <END DATE>. By leveraging a series of attacks, <YOUR NAME> found critical level vulnerabilities that compromised the exam environment and passing objectives. It is highly recommended that <CLIENT> address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Testing Summary

<Describe the vulnerabilities noted and basic information about impact of exploitation>

The following table describes how <YOUR NAME> <DESCRIBE THE OVERALL GOAL FOR EXAM COMPLETION>:

Step	Action	Recommendation
1	Actionable step taken	▪ Remediation 1 ▪ Remediation 2
1	Actionable step taken	▪ Remediation 1 ▪ Remediation 2
1	Actionable step taken	▪ Remediation 1 ▪ Remediation 2
1	Actionable step taken	▪ Remediation 1 ▪ Remediation 2
1	Actionable step taken	▪ Remediation 1 ▪ Remediation 2

Security Strengths

Strength

Strength Description

Strength

Strength Description

Copyright © <YOUR NAME>

Security Weaknesses

Weakness

Weakness Description

Weakness

Weakness Description

Weakness

Weakness Description

Copyright © <YOUR NAME>

Penetration Test Findings

IPT:001 – Finding Name

Description:	Include a brief description of the issue found
Systems:	Include the URL(s) or IP(s) affected
Severity:	Match Severity with the Severity Table
Tools Used:	List the tool(s) used for the finding
References:	List appropriate research references for the issue

Exploitation Proof of Concept

Figure 1: <DESCRIBE IMAGE>

(note that the 1: here updates across the document via right clicking and updating field)

Remediation

<INCLUDE STEPS TO REMEDIATE THE ISSUE>

Copyright © <YOUR NAME>

WPT:002 – Finding Name

Description:	Include a brief description of the issue found
Systems:	Include the URL(s) or IP(s) affected
Severity:	Match Severity with the Severity Table
Tools Used:	List the tool(s) used for the finding
References:	List appropriate research references for the issue

Exploitation Proof of Concept

Figure 2: <DESCRIBE IMAGE>

(note that the 1: here updates across the document via right clicking and updating field)

Remediation

<INCLUDE STEPS TO REMEDIATE THE ISSUE>

Copyright © <YOUR NAME>

EPT:003 – Finding Name

Description:	Include a brief description of the issue found
Systems:	Include the URL(s) or IP(s) affected
Severity:	Match Severity with the Severity Table
Tools Used:	List the tool(s) used for the finding
References:	List appropriate research references for the issue

Exploitation Proof of Concept

Figure 3: <DESCRIBE IMAGE>

(note that the 1: here updates across the document via right clicking and updating field)

Remediation

<INCLUDE STEPS TO REMEDIATE THE ISSUE>

Copyright © <YOUR NAME>

THIS PAGE LEFT INTENTIONALLY BLANK

Copyright © <YOUR NAME>